WHAT IS CLAIMED

[C01] A system for processing a transaction comprising:

a teller comprising an imaging device adapted to a) obtain an image of one or more than one transaction document, and b) optionally (i) recognize one or more field within the document and extract information from the fields and (ii) digitally sign each electronic transaction, and an optional station interconnected to the imaging device and adapted to receive the image and the optional information, the station adapted to a) input information, b) view the image and information c) store the image and information;

a local server comprising a synchronization agent and interconnected to one or more than one teller and adapted to receive the image and information, said local server further adapted to 1) detach the image from the information, 2) create an image file and an information file, 3) digitally sign each file and or the transaction, and 4) store the image file and the information file;

a central server comprising means for storing files and interconnected to one or more than one local server, said central server adapted to receive the image file and the information file, said local server transmitting the information file to the central server in real time and transmitting the image file to the central server in one of a) in real time and b) as determined by the synchronization agent, said central server adapted to a) validate the digital signatures, b) optionally combine the information file and the corresponding image file to recreate the electronic transaction, c) timestamp the information file, d) optionally transmit the timestamp to

the local server and e) identify a target for the electronic transaction, said central server optionally interconnected to the target by a network, said central server requesting one or more service from the network target and optionally transmitting the electronic transaction to the network target.

[C02] The system of claim 1 wherein each interconnection is one of an Internet, an Intranet, a direct link, wireless, a network, and a private portal.

[C03] The system of claim 1 wherein the teller is one of a teller window, a branch, a point-of-presentment, a point-of-sale, a kiosk, an ATM, a cash vault, a merchant, a corporate location, and an end user.

[C04] The system of claim 1 wherein the teller comprises a teller identifier.

[C05] The system for processing a transaction of claim 4 wherein the central server identifies the information file by the identifier.

[C06] The system of claim 4 wherein the identifier is one or more of a routing transit identifier, a routing transit number, a teller ID, a branch ID, a bank ID, the station ID, a date, a time, a transaction type, a transaction number, a batch number, a network node identifier, and a sequence number.

[C07] The system of claim 1 wherein the teller is adapted to perform a sign-on function.

[C08] The system of claim 7 wherein the identifier is initiated by the sign-on.

[C09] The system of claim 7 wherein the sign-on determines an amount of cash on hand in a cash drawer.

[C10] The system of claim 9 wherein one or more amount of cash on hand in a cash drawer are combined.

[C11] The system of claim 7 wherein the sign-on is one of electronic or manual.

[C12] The system of claim 7 wherein the sign-on is one of a username/password combination, a biometric, and a voice print.

[C13] The system of claim 1 wherein the teller constructs one or more associated document.

[C14] The system of claim 13 wherein the associated document comprises a teller identifier.

[C15] The system of claim 13 wherein the associated document is constructed from information received during a period of time.

[C16] The system of claim 13 wherein the associated document is one of a cash-in ticket and a cash-out ticket.

[C17] The system of claim 1 wherein the teller performs one or more function selected from the group an account look up, account status, validation of owner, availability of funds, determination of valid transaction document number, confirmation that a transaction document has not been previously presented, debit an account, credit an account, and memo post.

[C18] The system of claim 1 wherein the teller identifies each type of transaction.

[C19] The system of claim 18 wherein the transaction is selected from the group consisting of cashing a check, creating a cash letter, cash in ticket, cash out ticket,

payment coupon, data validation, identity validation, biometric capture, and making a cash deposit.

[C20] The system of claim 1 wherein the system is adapted to provide one or more function from the group consisting of image and information quality assurance, exception processing, security provision, audit, journaling, and image recall.

[C21] The system claim 1 wherein the information comprises a MICR line and an amount of a financial transaction.

[C22] The system of claim 1 wherein each digital signature comprises a unique algorithm.

[C23] The system of claim 22 wherein the unique algorithm consists of one or more of network specifics, user specifics, operator specifics, image specifics, file specifics, time specifics, transaction specifics, terminal specifics, and quality assurance specifics.

[C24] The system of claim 1 wherein the successful validation of the digital signatures by the central server is a verification that the files have not been altered and or were transmitted from a known source.

[C25] The system of claim 1 wherein a failed validation of one of the digital signatures by the central server determines that the electronic transaction has been subjected to unauthorized access and or transmitted from an unknown source.

[C26] The system of claim 1 wherein the central server comprises one or more configurable sorting and routing algorithm adaptable to forward the files to the target.

[C27] The system of claim 26 wherein the target is one or more of a network node, a printer, a database, a validation service, a security service, clearing and settlement.

[C28] The system of claim 26 wherein the sorting and routing algorithm is constructed from one or more of a routing transit number, transaction document type, bank ID, account ID, payee ID, user ID, user password, time, network node identifier and teller ID.

[C29] The system of claim 26 wherein the sorting and routing algorithm is constructed pursuant to a Direct Debit Authorization between at least two bank accounts.

[C30] The system of claim 27 wherein the target is a validation service and wherein the teller may optionally override validation.

[C31] The system of claim 30 wherein the override is initiated by electronic or manually input of a value.

[C32] The system of claim 31 wherein the value determines an endpoint for the transaction.

[C33] The system of claim 32 wherein the endpoint is an exception processing.

[C34] The system of claim 33 wherein the exception processing is standard paper transaction processing.

[C35] The system of claim 27 wherein the validation service is one of a service located at the central server, a network of banks, a contracted service that interfaces with banks, and a Shared Multi-Function Service Network.

[C36] The system of claim 27 wherein the validation service is adapted to a) compare an item listed in the information file to stored data, and b) return a response that the item is or is not a match.

[C37] The system of claim 36 wherein the item is one of an account number, an amount, an item number a name, a unique identifier, identifier for authorization, and an identifier for identification.

[C38] The system of claim 1 wherein the image file is printed as an image replacement document (IRD) as a substitute for the transaction document.

[C39] The system of claim 38 wherein the IRD meets industry standards and procedures relating to transaction document processing.

[C40] The system of claim 39 wherein transaction document processing is one of capture, transmission, synchronization, notification, presentment, clearing, settlement, adjustment of a cash letter, a deposit transaction, transaction of information, re-presentment, exception processing, reporting, validating, archiving, retrieval, a credit card transaction, a debit card transaction, manipulating a line of credit, a smart card transaction, privacy and security.

[C41] The system of claim 38 wherein the IRD is archived at any step in the transaction document processing.

[C42] The system of claim 38 wherein the IRD is transmitted to a transaction document owner.

[C43] The system for processing a transaction of claim 1 wherein one or more information file is used to create an account statement.

[C44] The system of claim 1 wherein the image file is transmitted to and from the central server at a time that does not coincide with transmission of the information file.

[C45] The system of claim 44 wherein the time is determined when a predetermined network bandwidth is detected by a network traffic monitor.

[C46] The system of claim 44 wherein the transaction document is transmitted to a second facility prior to imaging.

[C47] The system of claim 1 wherein the transaction document is one of a check, a deposit slip, a cash letter, a cash in ticket, a cash out ticket, a payment coupon, a loan coupon, security and or privacy information, a credit card, a debit card, a line of credit, and a smart card.

[C48] The system of claim 1 operatively interconnected with a printer.

[C49] A method for processing a transaction comprising:

1) imaging one or more than one transaction document at a teller and effecting one of a) extracting information from the image and b) manually inputting information into an electronic format to create an electronic transaction;

2) optionally digitally signing the electronic transaction at the teller;

3) transmitting the electronic transaction to a local server interconnected the teller;

4) detaching the image from the information and optionally creating an image file and an information file at the local server;

5) digitally signing each file and or the transaction at the local server;

6) transmitting the files to a central server interconnected to the local server; said transmission of the files in real-time or as determined by a synchronization agent located at the local server; said image file and information file optionally transmitted to the central server at different times;

7) validating the digital signatures at the central server;

8) and where files are transmitted at separate times, a) timestamping the information file at the central server, b) transmitting the timestamp to the local server, c) transmitting the image file, and d) combining the information file with and the corresponding image file to recreate the electronic transaction at the central server;

9), identifying a target for the electronic transaction, said target optionally connected to the central server in a network; and,

10) optionally effecting one or more of storing, printing, archiving, retrevial, requesting one or more service from the target, and transmitting the electronic transaction to one or more identified target.

[C50] The method of claim 49 wherein each interconnection is one of wireless, an Internet, an Intranet, a direct link, a network, and a private portal.

[C51] The method of claim 49 wherein the teller is one of a teller window, a branch, a point-of-presentment, a point-of-sale, a kiosk, an ATM, a cash vault, a merchant, a corporate location, and an end user.

[C52] The method of claim 49 further comprising the step of creating a teller identifier.

[C53] The method of claim 51 further comprising the step of identifying the information file transmitted to the central server by the identifier.

[C54] The method of claim 53 wherein the identifier is one or more of a routing transit identifier, a routing transit number, a teller ID, a branch ID, a bank ID, the station ID, a date, a time, a transaction type, a transaction number, a batch number, a network node identifier, and a sequence number.

[C55] The method of claim 49 further comprising the step of sign-on at the teller.

[C56] The method of claim 55 wherein the identifier is created by the sign-on.

[C57] The method of claim 55 further comprising the step of determining an amount of cash on hand in a cash drawer.

[C58] The method of claim 57 wherein one or more amount of cash on hand in a cash drawer are combined.

[C59] The method of claim 55 wherein the sign-on is one of electronic or manual.

[C60] The method of claim 55 wherein the sign-on is one of a username/password combination, a biometric, and a voice print.

[C61] The method of claim 49 comprising the step of creating one or more associated document at the teller.

[C62] The method of claim 61 further wherein the associated document comprises a teller identifier.

[C63] The method of claim 61 further comprising the step of creating the associated document from information received during a period of time.

[C64] The method of claim 63 wherein the associated document is one of a cash-in ticket and a cash-out ticket.

[C65] The method of claim 49 further comprising the step of performing one or more of looking up an account, determining account status, validating an owner, determining an availability of funds, determining a valid transaction document number, confirming that a transaction document has not been previously presented, debiting an account, crediting an account, and posting a memo at the teller.

[C66] The method of claim 49 further comprising the step of identifying each type of transaction at the teller.

[C67] The method of claim 66 wherein the transaction is selected from the group consisting of cashing a check creating a cash letter, cash in ticket, cash out ticket, payment coupon, data validation, identity validation, biometric capture, and making a cash deposit.

[C68] The method of claim 49 further comprising the step of providing one or more of determining image and information quality assurance, exception processing, security, and recalling an image at the teller.

[C69] The method of claim 49 wherein the information comprises a MICR line and an amount of a financial transaction.

[C70] The method of claim 49 further comprising the step of creating the digital signature using a unique algorithm.

[C71] The method of claim 70 wherein the unique algorithm consists of one or more of network specifics, user specifics, operator specifics, image specifics, file specifics,

time specifics, transaction specifics, terminal specifics, and quality assurance specifics.

[C72] The method of claim 49 further comprising the step of verifying files have not been altered and or were transmitted from a known source by validating the digital signatures at the central server.

[C73] The method of claim 49 further comprising the step of sorting and routing files based on one or more algorithm adaptable to forward the files to the target.

[C74] The method of claim 73 wherein the sorting and routing algorithm is constructed from one of a routing transit number, time, network node identifier, transaction document type, bank ID, account ID, payee ID, user ID, user password, and teller ID.

[C75] The method of claim 73 wherein the sorting and routing algorithm is constructed pursuant to a Direct Debit Authorization between at least two bank accounts.

[C76] The method of claim 73 wherein the target is one or more of a network node, printer, a database, a validation service, a security service, clearing and settlement.

[C77] The method of claim 76 further comprising the step of overriding the validation service by the teller.

[C78] The method of claim 77 further comprising the step of initiating the override by an electronic or manual input of a value at the teller.

[C79] The method of claim 78 including the step of determining an endpoint for the transaction from the value.

[C80] The method for processing a transaction of claim 78 wherein the endpoint is an exception process.

[C81] The method for processing a transaction of claim 79 further comprising the step of processing the transaction by standard paper transaction processing.

[C82] The method of claim 76 wherein the validation service is one of a service located at the central server, a network of banks, a contracted service that interfaces with banks, and a Shared Multi-Function Service Network.

[C83] The method of claim 76 further including the steps of a) comparing an item listed in the information file to stored data, and b) returning a response that the item is or is not a match to the stored data.

[C84] The method of claim 83 wherein the item is one of an account number, an amount, an item number a name, a unique identifier, identifier for authorization, and an identifier for identification.

[C85] The method of claim 49 comprising the step of printing an image replacement document (IRD) from the image file as a substitute for the transaction document.

[C86] The method of claim 85 wherein the IRD meets industry standards and procedures relating to transaction document processing.

[C87] The method of claim 86 wherein transaction document processing is one of capture transmission, synchronization, notification, presentment, clearing, settlement, adjustment of a cash letter, a deposit transaction, transaction of information, re-presentment, exception processing, reporting, validating, archiving, retrieval, a credit

card transaction, a debit card transaction, manipulating a line of credit, a smart card transaction, privacy and security.

[C88] The method of claim 49 wherein the image file is translatable as an IRD and the IRD is archived.

[C89] The method of claim 88 in which the IRD is transmitted to a transaction document owner.

[C90] The method of claim 49 further comprising the step of creating an account statement from one or more information file.

[C91] The method of claim 49 further comprising the step of transmitting the image file to and from the central server at a different time than that of transmission of the information file.

[C92] The method of claim 91 further comprising the step of determining the time by meeting or exceeding a predetermined network bandwidth detected by a network traffic monitor.

[C93] The method of claim 49 further comprising the step of transmitting the transaction document to a second facility prior to imaging.

[C94] The method of claim 49 wherein the transaction document is one of a check, a deposit slip, a cash letter, a cash in ticket, a cash out ticket, a payment coupon, a loan coupon, security and or privacy information, a credit card, a debit card, a line of credit, and a smart card.

[C95] A system for limiting the access of a second participant in a network to a service or an electronic record of a first participant in the network comprising:

a network access control list, said network list storing one or more permission granted to one or more participant in the network; and

a first participant and second participant each interconnected to the network; said first participant creating and maintaining a first participant access control list; said first participant list storing one or more permission granted to one or more second participant; said first participant list granting the same or less than the permissions listed for the second participant on the network list; said first participant created permissions allowing one or more second participant access to one or more service and or record of the first participant.

[C96] The system of claim 95 wherein the network is a Shared Multi-Function Service Networks.

[C97] The system of claim 95 further comprising a network System of Record (SOR) comprising a data file for a) maintaining and mapping permissions granted to participants and b) creating a log of all participant activity on the network.

[C98] The system of claim 95 wherein the participants are banks and the service is real time transaction document processing.

[C99] The system of claim 95 wherein the service is one of non-repudiation, authentication, and authorization.

[C100] The system of claim 95 wherein the participant list is a subset of and independent of the network list.

[C101] The system of claim 100 wherein the first participant restricts a service granted to the second participant with no interaction with the network list.

[C102] The system of claim 95 wherein network permissions are enforced through a public key and private key infrastructure.

[C103] The system of claim 95 wherein each participant optionally adds and or deletes one or more permission granted to a second participant, said added or deleted permission being listed on the network list.

[C104] The system of claim 95 wherein a third participant is unaware of permissions granted by the first participant to the second participant.

[C105] The system of claim 95 wherein each participant maintains a log of a) attempted access to the service and or record of that participant, and b) the service and or record successfully accessed by the second participant.

[C106] The system of claim 105 wherein the log is used to support one of dispute resolution, security and anti-fraud measures.

[C107] The system of claim 95 wherein the network permissions and or the participant permissions are created using a rule hierarchy comprising one or more of a standard for the network, security, service level, and processing.

[C108] The system of claim 95 wherein permission is determined by matching a digital certificate of a requesting participant to a permission stored in a Lightweight Directory Access Protocol.

[C109] The system of claim 95 wherein the participant lists use Simple Object Access Protocol to encode the record transmitted in response to the request via Secured Sockets Layer before transmitting over the network.

[C110] The system of claim 95 wherein the permissions further comprise one or more of Web Services, MQ, Java Connector Architecture, Java Message Service, Remote Method Invocation (RMI), IIOP, FTP, SFTP, and Corba Services.

[C111] A method of limiting access of a second participant in a network to a service and or an electronic record of a first participant in the network comprising:

1) creating and maintaining a network access control list; said network list storing one or more permission granted to one or more participant in the network; and

2) creating and maintaining a first participant access control list, said first participant list storing one or more permission granted to one or more second participant, said first participant list granting the same or less permissions listed for the second participant on the network list; said first participant permissions allowing one or more second participant access to one or more service and or record of the first participant optionally through a firewall of the first participant.

[C112] The method of claim 111 wherein the network is a Shared Multi-Function Service Networks.

[C113] The method of claim 111 further comprising the steps of a) maintaining and mapping permissions granted to participants and b) creating a log of all participant activity on the network.

[C114] The method of claim 111 wherein the participants are one of banks and related services and the service is real time transaction document processing.

[C115] The method of claim 111 wherein the service is one of non-repudiation, authentication, and authorization.

[C116] The method of claim 111 wherein the participant list is a subset of and independent of the network list.

[C117] The method of claim 116 further comprising the step of restricting a service granted to the second participant with no interaction with the network list by the first participant.

[C118] The method of claim 116 wherein network permissions are enforced through a public key and private key infrastructure.

[C119] The method of claim 111 further comprising the step of adding and or deleting one or more permission granted to a second participant by a first participant; said added or deleted permission one of a permission listed on the network list.

[C120] The method of limiting access of claim 111 wherein a third participant is unaware of the one or more permission granted by the first participant to the second participant.

[C121] The method of claim 111 further comprising the step of logging a) attempted access to the service and or record of the participant by that participant, and b) the service and or record successfully accessed by one or more second participant.

[C122] The method of claim 121 wherein the log is used to support one of dispute resolution, security and anti-fraud measures.

[C123] The method of claim 111 further comprising the step of creating the network permission and or participant permission using a rule hierarchy comprising one or more of a standard for the network, security, service level, and processing.

[C124] The method of claim 111 further comprising the step of determining permission by matching a digital certificate of a requesting participant to a permission stored in a Lightweight Directory Access Protocol.

[C125] The method of claim 111 further comprising the step encoding the record transmitted in response to the request use Simple Object Access Protocol via Secured Sockets Layer before transmitting over the network.

[C126] The method of claim 111 further comprising the step wherein one or more permission further comprise one or more of Web Services, MQ, Java Connector Architecture, Java Message Service, Remote Method Invocation (RMI), IIOP, FTP, SFTP, and Corba Services.

[C127] A method of assuring the quality of an electronic transaction created from a document comprising:

1) establishing one or more standard;

2) precapturing information associated with a transaction;

3) capturing an electronic transaction of a document including an image and data relating to the document;

4) determining postcapture information from the electronic transaction;

5) determining a quality assurance value from one or more of the precaptured information, and capture information;

6) comparing the value to the standard with the result that the electronic transaction is determined to be acceptable where the value equals or exceed the standard and is rejected where the value is less than the standard.

[C128] The method of claim 127 using one or more than one attribute to determine the standard.

[C129] The method of claim 127 wherein the standard is established based on one of human collection, machine collection, and combined collection.

[C130] The method of claim 127 wherein the rejected electronic transaction is flagged for exception processing.

[C131] The method of claim 127 wherein the standard is determined by one of a single and a iterative collection of one of the image, the data, and the electronic transaction.

[C132] The method of claim 127 further comprising the step of depicting an acceptable electronic transaction.

[C133] The method of claim 132 wherein the depiction is a stamp of approval.

[C134] The method of claim 127 wherein the establishment of an acceptable or a rejected electronic transaction occurs at any step in the processing of the transaction.

[C135] The method of claim 134 wherein the step is one of presentment, capture, transfer, printing, clearing, settlement, dispute, storage, and retrieval.

[C136] The method of claim 127 wherein the document is one of a check, a deposit slip, a cash letter, a cash in ticket, a cash out ticket, a payment coupon, a loan coupon, security and or privacy information, a credit card, a debit card, a line of credit, and a smart card.

[C137] The method of claim 127 further comprising the steps of enhancing fraud detection and providing assurance to a recipient that use an electronic version of the transaction document that the electronic transaction is acceptable and unique..

[C138] The method of claim 127 wherein the standard meets that provided in the Check Truncation Act.

[C139] The method of claim 127 wherein meta data is used to determine the standard.

[C140] The method of claim 127 wherein the transaction document is destroyed after establishment of the acceptable image.

[C141] The method of claim 127 wherein established standards are used.

[C142] The method of claim 141 wherein the established standards are determined using one or more of any X9B standard and those listed in Table I.

[C143] The method of claim 127 wherein the standard is determined based on one or more of the type of transaction document and an image capture device ID.

[C144] The method of claim 127 wherein precapture information determines that the image device is not introducing an unacceptable error into a processing environment.

[C145] The method of claim 127 wherein the standard is determined based on one or more of established data about the document, image device, capture environment, and expected results.

[C146] The method of claim 145 wherein established data is related to the document and is one of a check, a deposit slip, a cash letter, a cash in ticket, a cash out ticket, a payment coupon, a loan coupon, security and or privacy information, a credit card, a debit card, a line of credit, and a smart card.

[C147] The method of claim 145 wherein the established data is on a check and is one or more of MICR string, location of the string, an expected size of the image file, Courtesy Amount Recognition, Legal Amount Recognition, a calibration item, a layout for Optical Character Recognition, and a layout for Intelligent Character Recognition.

[C148] The method of claim 145 wherein the established data relates to the image device and is one or more of a type of capture device, capture device identification, Capture Device Image Deviation, Signal to Noise Ratio, Peak Signal to Noise Ratio, Modulation Transfer Function, Mean Squared Error, Frequency Distribution, Root Mean Squared Error, Mean Absolute Error, an image file size, Capture Device Quality Index, a Capture Device Image Resolution, and a Capture Device Image Format.

[C149] The method of claim 145 wherein the established data is related to the capture environment and is one or more of a high speed line, a teller line, a point of sale terminal, an ATM, a date, a time, a location, a device, a process, an image storage format, and capture calibration data.

[C150] The method of claim 145 wherein the established data is related to the expected results and is one or more of a given Image Type Identification (ITID), CDID, expected Image Quality Index (IQI), expected Image Similarity Index (ISI), expected Image Capture Format (ICF), and expected Image Storage Format (ISF) with file attributes.

[C151] The method of claim 127 further comprising the step of subjecting a rejected electronic transaction to exception processing.

[C152] The method of claim 127 wherein acceptable electronic transactions are digitally signed and or watermarked.

[C153] The method of claim 127 wherein the document is a check, the data collected is at least one of a check number and an account number and an operator manually inputs at least one of a visually perceived check number and account number, the image is an acceptable electronic transaction where the data collected matches the input data.

[C154] The method of claim 127 wherein an acceptable electronic transaction assures that 1) the electronic transaction was captured accurately and an adequate replacement document can be created; 2) critical data needed for legal precedent is captured and can be recreated; 3) the electronic transaction is the original and has not been tampered with; 4) an audit trail associated with the capture, manipulation and transmission of all data has been created; and 5) the image and data have been uniquely associated.

[C155] A system for receiving and processing an electronic transaction comprising:

an application comprising a synchronization agent and adapted to receive data related to at least one paper document representing an electronic transaction, said data comprising an image and information associated with the document, said application further adapted to 1) create an image file and a file comprising information associated with the document from the data, 2) digitally sign each file and or the data, and optionally 3) store the image file and or the file comprising information associated with the document; and

a server interconnected to the application, said server configured to receive the image file and the file comprising information associated with the document, said application transmitting the image file and or the file comprising information associated with the document to the server in one of 1) in real time and 2) as determined by the synchronization agent, said server adapted to validate the digital signatures and, where the file comprising information associated with the document is sent in real time and the image file is sent as determined by the synchronization agent, 1) timestamp the file comprising information associated with the document, 2) transmit the timestamp to the application where the application applies the timestamp to the image file, and 3) combine the file comprising information associated with the document and the image file when the image file is received at the server to consolidate the data, said server identifying and routing the file comprising information associated with the document and or the consolidated data to a target.

[C156] The system of claim 155 wherein the server is interconnected to the target by a network, said server requesting services from the target and or transmitting the

file comprising information associated with the document and or the recreated electronic data to the target.

[C157] The system of claim 95 wherein the participant created permissions pass through a firewall.

[C158] The method of claim 127 wherein the standard is one of a single value and a range of values.

[C159] The method of claim 127 wherein the standard is created using one or more of IQV, ITID, IQI, CDI, CDQI, ISI, CDID, IDCR, ICF, ISF, MDCI, MDCV, QACI, and QACV.

[C160] The method of claim 127 wherein the acceptability is determined by one of a single and a iterative collection of comparing the value to the standard.

[C161] The method of claim 159 wherein the acceptability is determined by one of a single and a iterative collection of comparing the value to the standard.

[C162] The method of claim 151 wherein exception processing is one of 1) additional imaging and or 2) additional manual or machine based quality assurance and or 3) flagging the transaction document for paper processing.

[C163] The method of claim 127 wherein the captured image is segmented into a grid and QA is performed on one or more than one element and or a subset of elements identified in one or more than one segment of the grid.

[C164] A secured multi-function shared services network for processing an electronic transaction comprising:

at least one participant having one or more service and or record necessary to process an electronic transaction; and

one or more integration node, each linked to participants, said node creating a secured multi-function shared services network by restricting access of said service and or record to the participants.

[C165] The network of claim 164 wherein the node provides one or more of authentication, authorization, non-repudiation, and or encryption.

[C166] The network of claim 165 wherein authentication is a public key infrastructure (PKI) and the integration node 1) issues and manages a PKI certificate to the participant making a request not restricted by any security restriction or additional security restriction, 2) digitally signs and verifies each PKI certificate, and 3) logs all PKI certificates used.

[C167] The network of claim 165 wherein the node provides authorization by 1) verifying one or more request and or response by matching the request and or response to an allowed service definition specific and unique to the participant offering the service, 2) storing and managing the known service definitions in a directory of services, and 3) logging each non-verified and verified request and or response.

[C168] The network of claim 165 wherein the node provides non-repudiation by issuing a certificate unique to the electronic transaction and tracking and logging all allowed and restricted services used for the transaction and or the associated certificate.

[C169] The network of claim 165 wherein the node provides encryption supported by https / secured sockets layer for secure transmission of the transaction to an un-trusted network.

[C170] The network of claim 164 wherein the integration node performs one or more function selected from 1) maintaining a log of all attempts for access to a participant and all requesters allowed to access a participant, 2) implementing services to requesters not restricted by any security restriction or additional security restriction, 3) implementing integration services to an existing system of one or more participant, 4) providing network administrative services and 5) compiling and providing network reports.

[C171] The network of claim 164 wherein the electronic transaction includes one or more of processing a check, a credit card transaction, a debit card transaction, a loan, a smart card transaction, and an information transaction.

[C172] The network of claim 171 wherein the electronic transaction is a check and the processing is one or more of writing, receiving, capturing, clearing, settling, transmitting, synchronizing, re-presenting, exception processing, reporting, validating, archiving, printing and retrieving.

[C173] The network of claim 171 wherein the electronic transaction is an information transaction consisting of comparing one of a name and or an identifier to a known list.

[C174] The network of claim 164 wherein the integration node performs one or more service consisting of 1) a security proxy and interface, 2) creating and or implementing one or more standard for the network, 3) providing a providing a public

key infrastructure (PKI), and 4) updating and or synchronizing the additional security restrictions.

[C175] The network of claim 174 wherein the standard is used for one of network security, messaging, logging, providing shared services, determining and or optimizing network performance, providing the PKI, providing web services, and or exception handling, reporting and management.

[C176] The network of claim 164 wherein the participant determines one or more unique additional access restriction to its services and or records through its node.